UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
---------- x

UNITED STATES OF AMERICA :

- v. - :

Taleek Brooks : **12 CR 166 (RRM)**

Defendant. :

----------x

DEFENDANT'S MEMORANDUM OF LAW
IN SUPPORT OF HIS MOTION TO SUPPRESS

Federal Defenders of New York
Michael D. Weil, Esq.
Ari Rosmarin, Law Student Intern
Attorney for Defendant
One Pierrepont Plaza
Brooklyn, New York 11241
Tel.: (718) 407-7413

TO: **Loretta Lynch, Esq.**
United States Attorney
Eastern District of New York
Attention: **AUSA Robert Polemeni**

TABLE OF CONTENTS

Page

Defendant Taleek Brooks submits this memorandum of law in support of his motion to suppress evidence recovered during the search of his computer over a closed file-sharing network on December 29, 2011, as well as evidence subsequently recovered pursuant to a search warrant based on the initial illegal search, and statements made on the date of his arrest.

PRELIMINARY STATEMENT

This case raises the fundamental question of whether law enforcement agents may randomly deceive citizens into "friending" them online, for the sole purpose of conducting exploratory searches of their home computers, repositories of information often more private than the home itself. Probable cause and a warrant must be required before the police target individuals online if the Fourth Amendment is to maintain its relevancy as a check against government overreach. Because law enforcement sought to befriend Mr. Brooks online with no warrant and no probable cause, and did so with the ultimate goal of rummaging through his computer, the evidence in this case must be suppressed.

Mr. Brooks was a member of GigaTribe, a closed peer-to-peer social network in many ways similar to the better-known Facebook. Participants share their most intimate items over these networks, but only with chosen friends. The networks thus remain a private sphere, like the home, open only to invited guests. The private nature of GigaTribe, as opposed to open file-sharing networks, distinguishes this case from those in which searches over file-sharing networks have been upheld against Fourth Amendment challenges.

The defendant accepted an undercover agent's "friend request," leading to a search of his files. As detailed below, this consent, predicated on a misrepresentation, was invalid and did not justify the search. Case law permitting the use of deception to gain entry into premises operating as a criminal enterprise does not allow a ruse for the sole purpose of a search.

Accordingly, the search of Mr. Brooks' computer, as well as evidence obtained pursuant to a search warrant wholly predicated on this initial search, must be suppressed.

STATEMENT OF FACTS

Social Networking

Nearly two-thirds of Americans who use the Internet participate in social networks.[1] Of these, more than two hundred million Americans use Facebook.[2] While each social network functions differently, social networking generally involves "the use of Web sites or other online technologies to communicate with people and share information, resources, etc."[3] Americans use social networking sites to stay in touch with current friends and family members, to connect with old friends with whom they've lost touch, to connect with others around a shared hobby or interest, to make new friends, to find romantic partners, and to read comments by public figures, among other reasons.[4] While some social networks facilitate the sharing of photographs and messages (e.g., Facebook), others are designed to assist in making new friends (e.g., Friendster), to facilitate professional connections (e.g., LinkedIn), share music tastes (e.g., Last.fm), make romantic connections (e.g., Match.com), participate in religious practice (e.g., HeavenUp), engage in political activities (e.g., TellMyGov), or to share computer files (e.g., GigaTribe).

---

[1] As of February 2012, 66 percent of Americans online participated in social networking. *See* Joanna Brenner, *Pew Internet: Social Networking (full detail)*, Pew Internet & American Life Project, May 31, 2012, *available at* http://pewInternet.org/Commentary/2012/March/Pew-Internet-Social-Networking-full-detail.aspx.

[2] At the end of 2011, 200 million Americans, or approximately two-thirds of the U.S. population, used Facebook. Jenna Wortham, "The Facebook Resisters," NY Times, Dec. 14, 2011, page B1. See http://www.nytimes.com/2011/12/14/technology/shunning-facebook-and-living-to-tell-about-it.html.

[3] *Social Networking Definition*, DICTIONARY.COM, http://dictionary.reference.com/browse/social+networking?s=t&ld=1032 (last visited Jul. 17, 2012).

[4] *See* Aaron Smith, *Why Americans use social media*, Pew Internet & American Life Project, Nov. 15, 2011, *available at* http://pewInternet.org/Reports/2011/Why-Americans-Use-Social-Media.aspx.

Social networking has become fully integrated into many Americans' lives. As of 2011, over 46 million Americans were logging into their social networking sites multiple times per day.[5] Yet while each social networking platform is crafted differently, many sites give users direct control over how much information to reveal and to whom. On Facebook, one privacy setting allows a user to mutually agree to become "friends" with another user, thus allowing both parties access to content from the other that would otherwise be inaccessible to each party.[6] If the parties so choose, once they are "friends," that level of access remains unless one party changes the level of access granted to that individual or to his or her "friends" in general.[7] The "friends" content-management concept exists in varying forms in a wide array of social networking sites, including GigaTribe.[8]

File-Sharing

One variety of social networking is file-sharing. While in previous eras of computer usage, individuals would share computer content by copying the information onto a floppy disk or CD-ROM and giving that disk to a friend or associate, technology now allows for such content to be shared directly over the Internet without the need for disks. File-sharing can take place over a variety of platforms, each with their own unique features, but one popular method is over "peer-to-peer" file-sharing networks.

A "peer-to-peer" file-sharing network typically allows anyone using the same computer software to view and download computer files from a shared folder on another user's computer

[5] Tom Webster, THE SOCIAL HABIT II at 3, Edison Research, 2011, *available at* http://www.slideshare.net/webby2001/the-social-habit-2011-by-edison-research.
[6] *See generally Friends*, FACEBOOK.COM, *available at* http://www.facebook.com/help/friends (last visited Jul. 17, 2012)
[7] *Id.*
[8] These include: Twitter (followers), MySpace (friends), Tumblr (followers), LinkedIn (connections), Last.fm (friends), Match.com (matches), GigaTribe (contacts), etc.

over the Internet, without individualized permission. See United States v. Sawyer, 786 F. Supp. 2d 1352, 1354 (N.D. Ohio 2011) (explaining open and closed peer-to-peer file sharing networks). Popular peer-to-peer file sharing networks of this type include LimeWire, Kazaa, and BitTorrent. A study in 2011 found that approximately 20 percent of total Internet bandwidth usage in the United States consisted of peer-to-peer file-sharing traffic.[9] Open peer-to-peer networks do not allow users to limit access to their shared content to other users of their selection; they only allow for general access to others on the network or others using the program.

GigaTribe

GigaTribe is a program that allows users to share files on their computer hard drives over the Internet with other users on their private network, only once both users have agreed to become "friends" on the program. It is a private, *closed* peer-to-peer file-sharing network, which gives users the ability to keep their files private from everybody but those to whom they individually grant access.[10] According to GigaTribe, "[s]ecurity is, of course, GigaTribe's major concern … Only the people [users] have invited can see [their] files … Only the folders [users] have selected are visible to [their] contacts … Every exchange is strongly encrypted: No one can see what is being shared."[11] The program has nearly 1.9 million users.[12] GigaTribe exists to allow users the opportunity to "quickly and privately share files of any size with people [they] rely on, family and associates."[13]

---

[9] *See Technical report: An Estimate of Infringing Use of the Internet* at 3, Envisional Ltd., Jan. 2011, *available at* http://documents.envisional.com/docs/Envisional-Internet_Usage-Jan2011.pdf.

[10] According to media reports, "GigaTribe is much like other file-sharing sites on the Web that are being monitored by the RIAA and MPAA, *but it creates a private network to keep them out*." *See* Don Reisinger, GigaTribe brings private P2P sharing to U.S., CNET.com (Nov. 17 2008, 11:33 AM), *available at* http://news.cnet.com/8301-17939_109-10098756-2.html.

[11] See Gigatribe.com, *available at* http://www.Gigatribe.com/en/product (last visited June 15, 2012, 1:11 PM)

[12] See Gigatribe.com (last visited June 15, 2012, 12:58 PM), *available at* http://www.Gigatribe.com/en/home.

[13] *GigaTribe FAQ, available at http://www.gigatribe.com/en/help-hosting-gigatribe (last visited June 28, 2012 3:11 PM).*

GigaTribe is thus in some ways a hybrid of a social network, like Facebook, and a file-sharing network, like Limewire. Although a participant chooses his or her friends, as with Facebook, once a person is accepted as a friend they have access to their friends' entire computer, not only selected items that are "uploaded" to the site.

Technologically, GigaTribe is different from Facebook in one significant regard insofar as it relates to this case. A person can access his or her Facebook account from any computer because the photos and data uploaded are maintained on a central server. On a private file-sharing network like GigaTribe, data always remains on your own computer, and when you download information from someone else's computer you do so through a direct connection between the two computers. (See Affidavit in Support of Search Warrant ¶ 13 ("SW Aff."), annexed as Ex. A to the Declaration of Michael D. Weil ("Weil Dec.")).

The Search of Mr. Brooks' Computer

On December 29, 2011, Taleek Brooks was a member of GigaTribe under the username "Tri-star." (See Brooks Dec. ¶ 2.) He had previously received a "friend" request from a user named "EvilBoy," which he accepted on or about December 24, 2011. (Weil Dec. ¶ 3.) "EvilBoy" was in fact an undercover FBI Agent. (Id.) The undercover agent proceeded to browse through Mr. Brooks' computer files. (SW Aff. 21-22.) For approximately nine minutes before any online chat took place between Mr. Brooks and the undercover agent, the agent searched through and attempted to download files from Mr. Brooks' computer. (Weil Dec. ¶ 3.) While Mr. Brooks ultimately engaged in a chat with the undercover agent discussing child pornography, the Agent had access to, and had viewed, Mr. Brooks' files before any such conversation took place. (Id.)

On January 10, 2012, FBI Agent Thomas Thompson obtained a search warrant authorizing the search and seizure of any computers and storage devices located at 934 Lafayette Avenue, 3rd Floor, Brooklyn, New York, which he had determined was the physical address associated with Tri-star. (SW Aff.)

The search warrant was authorized on January 10, 2012 and executed on January 13, 2012. (Complaint, 12-M-38, Weil Dec. Ex. B.) Mr. Brooks waived his Miranda rights and made incriminating statements on January 13, including that he shared child pornography over GigaTribe, and was arrested. (Id.) He was released on bond and subsequently re-arrested after a search of his computers, authorized by the warrant, revealed additional child pornography which he allegedly produced. (See Complaint 12-M-133)

Mr. Brooks stands charged with seven counts of production of child pornography, four counts of distribution of child pornography, and one count of possession of child pornography, all in violations of 18 U.S.C. §§ 2251(a), 2252(a)(2), and 2252(a)(4).

LEGAL BACKGROUND

The Fourth Amendment

The Fourth Amendment provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated … ." U.S. Const., amend. IV. The Fourth Amendment proscribes warrantless searches unless they fall under one of certain well-defined exceptions. See Smith v. Ohio, 494 U.S. 541, 542 (1990); United States v. Oguns, 921 F.2d 442, 446 (2d Cir. 1990) (referring to "the axiom that warrantless searches are per se unreasonable, subject to a few well-delineated exceptions") (citations omitted). The burden is on the government to establish an exception to the warrant

requirement applies. United States v. Perea, 986 F.2d 633, 639 (2d Cir. 1993).

The *Katz* Standard

An individual is entitled to the protections of the Fourth Amendment if she has (1) a subjective expectation of privacy in what is searched; and (2) an objective expectation of privacy that society is prepared to recognize as reasonable. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). While there is no clear standard for what makes such an expectation reasonable, the Supreme Court has focused on "everyday expectations of privacy that we all share." Minnesota v. Olson, 495 U.S. 91, 98 (1990) (holding that an overnight guest has a reasonable expectation of privacy while on the premises). The Supreme Court has also recognized as reasonable expectations of privacy in filing cabinets, see United States v. Ortega, 480 U.S. 709, 724 (1986) (doctor had reasonable expectation of privacy in office filing cabinet that he did not share with other employees); sealed parcels, see United States v. Jacobsen, 466 U.S. 109, 114 (1983) ("Letters and other sealed packages are in the general class of effects in which the public at large has a legitimate expectation of privacy; warrantless searches of such effects are presumptively unreasonable."); and locked containers, see United States v. Chadwick, 433 U.S. 1, 11 (1977) (holding that one who safeguards his personal possessions in a locked footlocker is due the protection of the Fourth Amendment).

It is at this point beyond dispute that the Fourth Amendment protects the home computer. United States v. Lifshitz, 369 F.3d 173, 190 (2d Cir. 2004).

The Recent *Jones* Decision

For years after Katz was decided, it was commonly understood that the reasonable expectation of privacy test was the sole means of determining whether an individual's interests were protected by the Fourth Amendment warrant requirement. Yet the Supreme Court's

decision in Jones v. United States, 132 S. Ct. 945 (2012), has re-invigorated pre-Katz property-based Fourth Amendment analyses.

In Jones, the government placed a GPS tracking device on the undercarriage of Mr. Jones' Jeep and tracked the vehicle's movements for 28 days, generating more than 2,000 pages of data, all conducted outside of the scope of a warrant issued by the district court for surveillance of Mr. Jones' vehicle. Id. at 948. The government used the data generated by the tracking device to obtain an indictment against Mr. Jones and several co-conspirators for conspiracy to distribute and possession with intent to distribute cocaine. Id. Mr. Jones was ultimately convicted in 2007 of the conspiracy charge and was sentenced to life in prison. Id. at 949. On appeal, the D.C. Circuit Court of Appeals reversed the conviction because the evidence gathered by warrantless GPS surveillance of Mr. Jones' vehicle was obtained in violation of the Fourth Amendment. See United States v. Maynard, 615, F.3d 544 (D.C. Cir. 2010). The government appealed to the Supreme Court.

The Supreme Court voted 9 to 0 to affirm the D.C. Circuit's decision that the government's surveillance was unconstitutional. Justice Scalia wrote an opinion for five members of the Court, holding that the government's installation of a GPS device on Mr. Jones' vehicle and the use of that device to obtain information was a Fourth Amendment search under pre-Katz common law trespass Fourth Amendment analysis, and thus probable cause and a warrant was required. Id. at 949-950 ("[F]or most of our history the Fourth Amendment was understood to embody a particular concern for government trespass upon the areas ('persons, houses, papers, and effects') it enumerates. *Katz* did not repudiate that understanding.")

Writing for four members of the court, Justice Alito wrote an opinion finding that the government's installation of the GPS device was a violation of the Fourth Amendment under the

Katz reasonable expectation of privacy test. Id. at 964. Justice Alito emphasized that the advancements in technology in recent years have made prolonged and invasive government surveillance "cheap and easy." Id. According to Justice Alito, warrantless surveillance in which the government "secretly monitor[s] and catalogue[s] every single movement of an individual's car for a very long period" impinges on reasonable expectations of privacy. Id.

Finally, Justice Sotomayor, who joined Justice Scalia's opinion and agreed with Justice Alito that the search violated the Katz standard as well, wrote a concurring opinion that emphasized the efficiency and scope of GPS surveillance. Id. at 955 ("GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations."). Justice Sotomayor also noted the ability of secret surveillance to chill associational and expressive freedoms, see Id. at 956, and questioned whether people would reasonably expect the Government to conduct surveillance that might reveal their "political and religious beliefs, sexual habits, and so on" without a warrant. Id.

Searches over File-Sharing Networks.

Several circuits have held that the government's act of downloading computer files from a citizen's computer through an *open* file-sharing program does not implicate the Fourth Amendment because use of file-sharing software in effect forfeits her expectation of privacy in the contents of her computer. See e.g. United States v. Ganoe, 538 F.3d 1117, 1127 (9th Cir. 2008) (defendant's expectation of privacy in his personal computer could not "survive [his] decision to install and use file-sharing software, thereby opening his computer to anyone else with the same freely available program."); United States v. Borowy, 595 F.3d 1045 1047-1048 (9th Cir. 2010) (same); United States v. Stults, 575 F.3d 834, 842-43 (8th Cir. 2009) (same);

United States v. Perrine, 518 F.3d 1196, 1204-05 (10th Cir. 2008) (same).

The defense has located only three district court cases – none from this circuit – concerning searches over GigaTribe. See United States v. Sawyer, 786 F. Supp.2d 1352 (N.D. Ohio 2011); United States v. Soderholm, 2011 WL 5444053 (D. Neb., Nov. 9, 2011); United States v. Ladeau, 2010 WL 147523 (D. Mass. April 7, 2010).[14] In each of these cases the Court upheld the searches. Notably, however, in two of the cases, the government obtained access to the defendant's computer files by logging on to GigaTribe with the permission of a third-party who was already a GigaTribe friend of the defendant; the courts upheld the searches under the "third-party disclosure doctrine," which holds that when a person reveals information to a third party, they assume the risk that the third party may disclose it to the Government. See Ladeau, 2010 WL at *4-5; Sawyer, 786 F. Supp.2d at 1356 (citing Smith v. Maryland, 442 U.S. 735, 743 (1979)).[15]

Undercover Operations and the Fourth Amendment.

As detailed above, this case involves the use of an undercover operation. While generally permitted, the government's ability to use deception to gain entry to a home, and by logical extension, a computer, is not without limit. In general, while courts have permitted agents to assume false identities, no court has given its approval to the use of deception to gain entry for the sole purpose of conducting an exploratory search. Thus in Lewis v. United States, 385 U.S. 206 (1966), an undercover agent was invited into the defendant's home to buy marijuana. The Court rejected the notion that the entry violated the Fourth Amendment. "During neither of his visits to petitioner's home did the agent see, hear, or take anything that

[14] We have located no cases concerning searches over Facebook.

[15] In the third case, the court's decision did not rule on the issue present in this case: whether the government may "friend" an individual online without probable cause for the sole purpose of conducting an exploratory search. See Soderholm, 2011 WL 5444053.

was not contemplated and in fact intended, by petitioner as a necessary part of his illegal business." Id. at 210. In such a scenario, "the home is converted into a commercial center to which outsiders are invited for purposes of transacting unlawful business, [therefore] that business is entitled to no greater sanctity than if it were carried on in a store, a garage, a car, or on the street." Id. at 211. By contrast, in Gouled v. United States, 255 U.S. 298 (1921), overruled on other grounds, Warden v. Hayden, 387 U.S. 294 (1967), an acquaintance of the defendant, at the discretion of authorities, pretended to pay a social visit to the defendant, but searched for and seized private papers while the defendant was out of the room. The Court found this to violate the Fourth Amendment. Id. In Gouled, the Court held that entrance by an agent of the Government "by stealth, or through social acquaintance, or in the guise of a business call … whether or not the owner be present or not when he enters, any search and seizure subsequently and secretly made in his absence, falls within the scope of the prohibition of the Fourth Amendment ... ." Id. at 306.

Thus, while an undercover agent may use deception to encourage the defendant to engage in a transaction within a home being used for illicit activities, he may not do so exclusively in order to obtain entry to search. See State v. Pi Kappa Alpha Fraternity, 23 Ohio St.3d 141 (1986) (citing Gouled). In Pi Kappa Alpha Fraternity, liquor control agents purported to be fraternity alumni to gain consent to enter a fraternity house, where they found a vending machine that sold beer. The agents subsequently relied on that search to obtain a warrant to search the house and charged the fraternity with various liquor offenses. Id. On a motion to suppress by the fraternity, relying on Gouled and Lewis, the court held that government agents may not deceptively gain warrantless entry to a private home or office when it is not a commercial center

of criminal activity and the invitation to enter was not extended for the purpose of conducting illegal activities. Id. at 145.

ARGUMENT

I.

The Agent's Warrantless Search of Mr. Brooks' Computer Was Unconstitutional.

A. The Agent's Friend Request Required Probable Cause and a Warrant.

The Fourth Amendment requires that this Court rule, as a matter of first impression, that the government's use of an online ruse – in this case a friend request – for the express purpose of gaining access to the defendant's computer, required probable cause and a warrant.

There is no doubt that Mr. Brooks maintained a reasonable expectation of privacy in the contents of his computer. Lifshitz, 369 F.3d at 190. Moreover, unlike those cases involving open file-sharing discussed above, Mr. Brooks did not install software on his machine that made this expectation unreasonable. See Ganoe, 538 F.3d at 1127. Rather, access to his computer was restricted to designated "friends." Just as inviting friends to one's home does not forfeit one's right to privacy, so too may one maintain a privacy interest in a computer the contents of which are shared with a select few. This case is also distinguishable from all but one of the cases concerning closed file sharing networks. In those cases, the police gained access to the defendant's computer by using the identity of a third party to whom the defendant had already granted access, which is a risk Mr. Brooks arguably assumed. See Ladeau, 2010 WL at *4-5; Sawyer, 786 F. Supp.2d at 1356. Instead, this case presents novel questions about law enforcement's use of the Internet.

The defendant in this case was not transacting any business. Thus, the ruse in this case was not an example of the police simply concealing their identity so that a suspect would engage

in a prohibited commercial transaction – something clearly permitted – that happened to take place in the defendant's home as in Lewis. Rather, this case is closer to Gouled in that the entire purpose of the ruse was to gain entry to search through the defendant's files. Here, the agent disguised himself as the defendant's GigaTribe "friend" and Mr. Brooks – perhaps believing that the user "friending" him was someone he knew – granted him access. From that point, the agent began looking through Mr. Brooks' computer hard drive files. No conversation took place between the agent and the defendant until after the agent sought and received the "friend status" that granted him this access. Crucially, the agent began searching through Mr. Brooks' computer well before any conversation about child pornography took place. (Weil Dec. ¶ 3.)

The potential significance of warrantless government access to a person's computer is enormous. Whereas traditionally the home and office were the storage locations for personal documents such as financial records, health records, personal correspondence, and diaries, most of those records are now stored on personal computers. See Katherine J. Strandburg, Home, Home on the Web and Other Fourth Amendment Implications of Technosocial Change, 70 Md. L. Rev. 614, 655 (2011). The notion that accepting a "friend" request could result in unchecked law enforcement access to this information begs for Fourth Amendment protection. A private online security firm conducted a study in 2009 finding that nearly half of Facebook users accepted friend requests from two Facebook accounts with fictional names created by the company, whose photographs identified one as a toy rubber duck and one as two cats lying on a rug. See Tom S. Noda, Facebook Still a Hotbed of Identity Theft, Study Claims, PCWorld.com.[16] Equally troubling, the Pew Internet & American Life Project found that

[16] *http://www.pcworld.com/article/184522/facebook_still_a_hotbed_of_identity_theft_study_claims.html.*

Facebook users are three times as likely as non-Internet users to feel that "most people can be trusted."[17]

Courts have for years emphasized the importance adapting the protections of the Fourth Amendment to the dramatic pace of enhanced technological surveillance capacity. See United States v. Olmstead, 277 U.S. 438, 472 (1928) (Brandeis, J. dissenting) (Constitutional clauses protecting individuals against abuses of power must have "capacity of adaptation to a changing world"); United States v. White, 401 U.S. 745, 770 (1971) (Harlan, J., dissenting) (describing the surveillance technology of 1971 reaching the feasibility of "Orwellian Big Brother"); Kyllo v. United States, 533 U.S. 27, 34 (2001) (evolving technology cannot be permitted to "erode the privacy guaranteed by the Fourth Amendment"); United States v. Pineda-Moreno, 617 F.3d 1120, 1126 (9th Cir. 2010) (noting in GPS tracking surveillance case that "[w]e are taking a giant leap into the unknown, and the consequences for ourselves and our children may be dire and irreversible. Some day, soon, we may wake up and find we're living in Oceania.")

The unanimous decision in the Jones GPS case is illustrative of courts' newfound willingness to consider the means in which Fourth Amendment doctrine must evolve to deal with new technology. Under traditional Fourth Amendment law the surveillance at issue in Jones would seem entirely lawful. One's movements in public are generally not protected. See, e.g., United States v. Knotts, 460 U.S. 276, 281 (1983) ("A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."). Acknowledging the traditional Fourth Amendment analysis, the Supreme Court in Jones recognized the significance of the evolving capacity of surveillance technology to gather

[17] Keith Hampton, et al, *Social Networking sites and our lives*, Pew Internet & American Life Project, June 16, 2011, *available at* http://www.pewInternet.org/Reports/2011/Technology-and-social-networks/Summary.aspx.

tremendous amounts of personal information from individuals with little expenditure of resources or time.

Justice Alito observed that "[i]n the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical … Devices like [GPS], however, make long-term monitoring relatively easy and cheap," thus requiring judicial oversight. Jones, 132 S. Ct. at 963-964 (2012) (Alito, J., concurring). It is the changed capacity of the surveillance technology to gather such extensive information about an individual that requires an extension of the Fourth Amendment.

Similarly, courts have recognized that technology's evisceration of practical limitations on data collection may require the creation of judicial limitations outside of the GPS context. In In the Matter of an Application for an Order Authorizing the Release of Historical Cell-Site Information, 809 F. Supp. 2d 113 (E.D.N.Y. 2011), the court concluded that the government's request for recorded information identifying cellular telephone base station towers and sectors that received transmissions from the targeted cellular telephone required a showing of probable cause, not the lesser showing embodied in the Stored Communications Act, 18 U.S.C. §§ 2703(c)(1), (d). The court found the information sought "capture[d] enough of the user's location information for a long enough time period … to depict a sufficiently detailed and intimate portrait of his movements to trigger" the same constitutional concerns that motivated the D.C. Circuit Court in Maynard, the GPS case that was later affirmed in Jones. Id. Judge Garaufis cited circuit court opinions that raised grave concerns about the prospect of the police conducting "'wholesale surveillance' by attaching [GPS] devices to thousands of random cars and then analyzing the volumes of data produced for suspicious patterns of activity." Id. at 119 (quoting United States v. Marquez, 605 F.3d 604, 610 (8th Cir. 2010)).

The capacity for newer technologies like GPS tracking and cell-site data to permit the government to gather significant quantities of data about individuals—potentially on a mass scale—has given courts good reason to extend Fourth Amendment protection to surveillance employing these technologies. This case is in many ways analogous to the GPS and cell-site data cases insofar as the technological elimination of practical limitations on surveillance creates the need for judicial limitations. Although this case does not involve temporally prolonged surveillance, the depth of invasion is in many ways greater; home computers are the central repository for personal information in the modern age and access to an individual's home computer has the capacity to reveal significantly more about that individual's whereabouts, interests, associates, beliefs, and secrets than prolonged tracking of an individual's car could reveal.

As in the GPS and cell-site cases, practical limitations previously prevented the sort of conduct at issue here. Assume, *arguendo*, that notwithstanding Gouled undercover agents could knock on the door of every home in the United States in the hope that a tiny percentage of respondents would accidentally open their doors a little too wide and reveal contraband inside. In practice, the police would never pursue this strategy. Limited resources cause the police to follow leads and leave most people alone.

Such wholesale strategies are simple, efficient and free to pursue over social networks. The government could send Facebook friend requests to 200 million Americans, and if half accepted the requests without qualification, as the study cited above suggests,[18] the government could simply browse through the photos of 100 million Americans in search of evidence of unlawful activity.

[18] *See n. 16 supra*.

If traditional Fourth Amendment doctrine allows this – and the defense submits Gouled prohibits it but the law has never been applied in this context – that doctrine must evolve. As noted by Justice Sotomayor in Jones about GPS surveillance, most Americans would never expect the government to be able to obtain such private information without a warrant. See Jones, 132 S. Ct. at 956 (Sotomayor, J., concurring). When faced with the tremendous number of Americans using social networking sites like Facebook and GigaTribe, the frequency with which social network users are willing give consent to strangers online, the potential amount of information about an individual accessible over social networks, and the long track record of government surveillance overreach, the carelessness of millions of social network users cannot become an open and limitless window for undercover law enforcement investigations. Allowing the traditional consent exception to the warrant requirement to apply in such a setting would undermine the Fourth Amendment's aspirations of preventing "a too permeating police surveillance." United States v. Di Re, 332 U.S. 581, 595 (1948)

This is not merely an abstract "parade of horribles." Law enforcement has embraced the absence of judicial oversight in this area with gusto. See, e.g., KJ Lang, "Facebook friend turns into Big Brother," La Crosse Tribune, Nov. 19, 2009 (student accepted Facebook friend request from a "good-looking girl" who in fact was undercover police officer resulting in a ticket for underage drinking)[19]; Julie Massis, "Is this lawman your Facebook friend?" Boston Herald (Jan. 11, 2009)[20] (noting that half of local police departments surveyed in 2009 reported using social networking websites in detective work); Junichi P. Semitsu, From Facebook to Mug Shot: How the Dearth of Social Networking Privacy Rights Revolutionized Online Government

[19] http://lacrossetribune.com/news/local/article_0ff40f7a-d4d1-11de-afb3-001cc4c002e0.html
[20] http://www.boston.com/news/local/articles/2009/01/11/is_this_lawman_your_facebook_friend/

Surveillance, 31 Pace L. Rev. 291, 322 (2011) (describing a Justice Department memorandum obtained by the Electronic Frontier Foundation which referenced federal agents' use of fake identities on Facebook to obtain evidence, search for evidence, and track suspects).

While surely technology is an important police tool, there is enormous potential for abuse. Given the powerful yet invasive nature of internet undercover investigations, and the enormous incentive for the police to undertake them, probable cause and a warrant should be required. While perhaps a statutory response to this type of invasive surveillance is desirable, currently "the Fourth Amendment remains the primary regime for regulating government information gathering." Daniel J. Solove, Fourth Amendment Pragmatism, 51 B.C.L. Rev. 1511, 1527 (2010).

B. The Defendant's Consent was Invalid Under *Jones*.

As a second and independent ground requiring suppression, the undercover agent's obtaining of consent by means of a misrepresentation was invalid under trespass law, which applies to the Fourth Amendment as re-established in Jones v. United States, 132 S. Ct. 945, 949 (2012).

In Jones, Justice Scalia, writing for five members of the Court, held that where "the Government obtains information by physically intruding on a constitutionally protected area … a search has undoubtedly occurred." Id. at 951, n.3. Here, the Government obtained information from Mr. Brooks' home computer, his personal effect over which he controlled exclusive access. Trespass analysis readily applies to unauthorized access to a computer. See Register.com, Inc. v. Verio, Inc., 356 F.3d 393, 438 (2d Cir. 2004) (district court's determination that use of search robot to access computer system without authorization was trespass); Theofel v. Farey Jones, 359 F.3d 1066 (9th Cir. 2004) (interpreting Stored Communications Act in light of common law

trespass tort); CompuServe Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1021 (S.D.Ohio 1997) ("Electronic signals generated and sent by computer have been held to be sufficiently physically tangible to support a trespass cause of action.")

Justice Scalia's invocation of a common law trespass analysis for purposes of Fourth Amendment search analysis in Jones draws upon a relevant and significant expanse of common law trespass jurisprudence. Although the Supreme Court has in the past rejected extensions of certain elements of trespass doctrine to the Fourth Amendment context, see, e.g., McGuire v. United States, 273 U.S. 95, 98 (1927) (holding doctrine of *trespass ab initio* should not be extended to Fourth Amendment analysis), the Jones court affirmatively restored trespass doctrine into Fourth Amendment analysis. See Jones, 132 S. Ct. at 953 ("What we apply is an 18th-century guarantee against unreasonable searches, which we believe must provide at a *minimum* the degree of protection it afforded when it was adopted.") (emphasis in original).

The search here would have been a trespass at common law because at common law consent to entry obtained by misrepresentation or mistake is often invalid. See Restatement (Second) of Torts § 173 ("A conscious misrepresentation as to the purpose for which admittance to the land is sought, may be a fraudulent misrepresentation of material fact"); Prosser and Keeton on the Law of Torts § 18 at 119 ("[A]n overt manifestation of assent would not be effective … if the defendant knew, or probably if he ought to have known in the exercise of reasonable care, that the plaintiff was mistaken as to the nature and quality of the invasion intended."); 75 Am Jur 2d Trespass § 76 ("Neither express nor implied consent constitutes a

viable defense to a trespass action, if it was obtained by misrepresentation or fraud");[21] Shiffman v. Empire Blue Cross and Blue Shield, 256 A.D.2d 131 (1st Dep't 1998).

Here, by misrepresenting himself as a fellow GigaTribe user, "Evilboy," the undercover agent misrepresented the purpose for his entry into Mr. Brooks' computer. The agent's purpose was not to exchange files or chat, but rather his express purpose was to conduct a search of Mr. Brooks' computer for contraband. Although Mr. Brooks was under the belief that he was granting his permission to an individual who intended to share files with him, the agent was aware of Mr. Brooks' misunderstanding and, in fact, relied on it in obtaining Mr. Brooks' consent to access his hard drive. This type of misrepresentation goes to the heart of the agent's misrepresentation in gaining Mr. Brooks' consent. Obviously Mr. Brooks would not have consented to the entry if he understood the agent's true purpose was an exploratory search of his files, rather than the ordinary GigaTribe usage of exchanging files or chatting.

As the Agent's misrepresentation meets the requirements for vitiating consent under traditional common law trespass analysis, Mr. Brooks' consent was not validly obtained. Under the Court's incorporation of common law trespass doctrine into Fourth Amendment search analysis in Jones, Mr. Brooks did not validly waive his Fourth Amendment protections.

C. **The Evidence Recovered Pursuant to the Warrant, and the Defendant's Statements, Must be Suppressed as Fruit of the Poisonous Tree.**

The fruit of the poisonous true doctrine requires exclusion of the "fruits" of illegally obtained evidence unless "granting establishment of the primary illegality, the evidence to which instant objection is made has been come at ... instead by means sufficiently distinguishable to be

[21] However, not all deceit vitiates consent. See Theofel v. Farey-Jones, 341 F.3d at 983. The mistake must "extend to the essential character of the act itself, which is to say that which makes it harmful or offensive, rather than to some collateral matter which merely operates as an inducement." Id. (quoting Prosser & Keeton § 13 at 70). Judge Kosinski noted in Theofel that the distinction is often "fine and incoherent." Id

purged of the primary taint." Wong Sun v. United States, 371 U.S. 471 (1963); see United States v. Trzaska, 111 F.3d 1019 (2d Cir. 1997) ("evidence obtained during an illegal search should not be included in a warrant affidavit.")

The government obtained a search warrant for Mr. Brooks' home and computer solely based on the initial illegal search. In the course of executing the search warrant, the agents obtained a confession from Mr. Brooks. All of this evidence – his statements and the evidence recovered from his computers – was the direct fruit of the initial illegal search over GigaTribe. No search warrant for the defendant's home would have issued but for the GigaTribe search, nor would the defendant have been questioned.

The fruit of the poisonous tree doctrine is not absolute; it "allows the receipt in evidence, despite law enforcement misconduct, of evidence that the government inevitably would have discovered legally in any case as well as evidence that is only tenuously connected to illegal government action. U.S. v. Ghailani,743 F. Supp.2d 242, 250 (S.D.N.Y. 2010). Here, the other evidence is plainly the un-attenuated fruit of the primary illegality. Accordingly, all the evidence recovered pursuant to the arrest and warrant must be suppressed.

CONCLUSION

For the foregoing reasons, the evidence in this case recovered over the Internet, from the defendant's computers and home, and his statements, must be suppressed.

Dated: Brooklyn, New York
July 26, 2012

FEDERAL DEFENDERS
OF NEW YORK

_____/s_____
Michael D. Weil, Esq.
Ari Rosmarin, Law Student Intern
One Pierrepont Plaza
Brooklyn, New York 11241
Tel.: (718) 407-7413

TO: **Loretta Lynch, Esq.**
United States Attorney
Eastern District of New York
Attn: AUSA Robert Polemeni